	Oblasť	Názov nástroja	Nainštalované u koho
1	SIEM	ELK Stack	BRAIN:IT + FRI
2	SOAR	Shuffle	FRI
3	EDR	Wazuh	BRAIN:IT + FRI
4	Skener zraniteľností	Greenbone Community edition	BRAIN:IT + FRI
5	CTI	OpenCTI	FRI
6		MISP	FRI
7	Asset management	GLPI	BRAIN:IT
8		NetBox	FRI
9	Ticketing	DFIR IRIS	FRI
10	Evidencia, správa incidentov	DFIR IRIS	FRI
11	Reporting	Kibana (ELK)	BRAIN:IT + FRI
12	Knowledge portál	Wiki.js	BRAIN:IT

Zodpovedná osoba
BIT
FRI - Uramová
BIT
BIT
FRI - Uramová
FRI - Uramová
BIT
FRI - Segeč
FRI - Uramová
FRI - Uramová
BIT
BIT

Oblasť / Funkcia (SOC)	Komponent (produkt)
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)
SOAR	Shuffle
EDR	Wazuh
Skener zraniteľností	Greenbone Community Edition (GVM)
CTI	OpenCTI
CTI	MISP
Asset management	GLPI
Asset management / IPAM/DCIM	NetBox
Ticketing	DFIR IRIS
Evidencia, správa incidentov	DFIR IRIS
Reporting	Kibana (ELK)
Knowledge portál	Wiki.js

Edícia / Verzia
podľa implementácie
podľa implementácie
podľa implementácie
Community
podľa implementácie
podľa implementácie
podľa implementácie
podľa implementácie
podľa implementácie
podľa implementácie
podľa ELK
podľa implementácie

Účel v SOCsaas
Centrálna agregácia, indexácia a korelácia logov + vyhľadávanie a analýza
Orchestrácia a automatizácia reakcií (playbooky)
Endpoint monitoring/detekcie a základná reakcia + posielanie udalostí do SIEM
Pravidelné skenovanie infra/servisov a reporting zraniteľností
Správa a korelácia threat intelligence, obohacovanie alertov/incidentov
Evidencia, zdieľanie a distribúcia IOCs/events, feedy pre detekcie
Evidencia aktív, CMDB/ITSM evidencia, väzba na vlastníkov a služby
Zdroj pravdy pre IP rozsahy, zariadenia, lokality, topológiu (podklad pre skeny a monitoring)
Správa ticketov a úloh SOC (triage, eskalácie, SLA)
Centrálna evidencia incidentov a dôkazov (case management)
Vizualizácie, dashboardy a reporty pre SOC a management
Znalostná báza (runbooky, postupy, playbooky, onboarding)

Kľúčové capability
ingest pipeline, normalizácia, vyhľadávanie, alerting (ak povolené), dashboards
workflow/playbooky, automatizácia krokov, integrácie, schvaľovania (podľa flow)
agent na koncových bodoch, FIM, detekcie, policy, alerting, základné response kroky
plánované skeny, CVE detekcia, reporty, scoring (CVSS)
STIX objekty, knowledge graph, konektory, enrichment
eventy, atribúty/IOCs, feedy, tagging, sharing
asset registry, životný cyklus, vzťahy, (voliteľne) helpdesk moduly
IPAM, DCIM, inventár, vzťahy, exporty
case/ticket workflow, priradenie, komentáre, SLA/tagy
evidovanie incidentov, artefakty, prílohy, časová os, chain-of-custody (ak používané)
dashboardy, vizualizácie, (voliteľne) report export
verzovanie stránok, šablóny, vyhľadávanie, prílohy

Vstupy (zdroje dát)
syslog, Windows eventy, aplik. logy, sieťové prvky, cloud logy, Wazuh alerts
alerty z ELK/Wazuh, CTI (OpenCTI/MISP), tickety z DFIR IRIS, webhooky
endpointy (agent), OS logy, integrity events
IP rozsahy z NetBox, assety z GLPI, manuálne ciele
CTI feedy, MISP, manuálne vloženie, externé zdroje
manuálne a automatické feedy, externé komunity, analýza incidentov
onboarding aktív, importy, (voliteľne) NetBox, manuálne záznamy
manuálne/automatické napĺňanie infra dát
alerty zo SIEM/SOAR, manuálne vytvorenie
tickety, dôkazy z vyšetrovania, exporty z ELK/Wazuh/Greenbone
indexy v Elasticsearch
dokumentácia SOC procesov, incident postupy

Výstupy (artefakty)
indexy/logy, detekčné pravidlá, alerty, dashboardy, reporty
spustené akcie, záznamy o vykonaní, obohatené incidenty/tickety
alerty, incident events, telemetria do SIEM
nálezy zraniteľností, reporty, exporty
TI entity, väzby, obohatené IOCs, exporty
IOC feedy pre SIEM/SOAR/EDR, exporty STIX/JSON/CSV
zoznam aktív, vlastníci, atribúty pre skeny/detekcie
IP rozsahy pre Greenbone, mapovanie infra pre SOC
tickety, stavovanie, audit trail
incidentné spisy, evidenčné záznamy, export pre audit
reporty, KPI dashboardy, exporty
interná dokumentácia, runbooky

Integrácie / API	Nasadenie
REST API, Beats/Agent, syslog, webhooky (podľa stacku)	self-hosted (VM/Docker/K8s)
REST API, webhooky, konektory	self-hosted (Docker/K8s)
Wazuh API, integrácia na Elastic/Logstash, syslog	self-hosted (manager + agents)
GMP API, exporty (CSV/XML), napojenie cez automatizáciu	self-hosted (VM/Docker)
REST/GraphQL API, konektory, STIX/TAXII (podľa modulov)	self-hosted (Docker/K8s)
REST API, exporty (STIX), možné TAXII (podľa konfigurácie)	self-hosted (VM/Docker)
REST API, import/export	self-hosted
REST API, webhooks	self-hosted
API, webhooky (podľa možnosti), integrácia so SOAR	self-hosted
API, import/export	self-hosted
REST API (Kibana/Elastic), integrácia v rámci ELK	súčasť ELK
LDAP/OIDC (podľa konfigurácie), API, Git sync (ak využité)	self-hosted

Uloženie dát / retencia
Elasticsearch storage; retencia konfigurovateľná
lokálna DB/logy o behu; retencia konfigurovateľná
Wazuh indexy/archív; retencia konfigurovateľná
lokálna DB so scan výsledkami; retencia konfigurovateľná
DB (napr. Elastic/Neo4j podľa setupu); retencia konfigurovateľná
DB udalostí/atribútov; retencia podľa politiky
DB; retencia podľa interných pravidiel
DB; retencia podľa interných pravidiel
DB prípadov; retencia konfigurovateľná
DB + úložisko príloh; retencia podľa politiky
dáta v Elasticsearch; retencia podľa SIEM politiky
DB + súbory; retencia podľa interných pravidiel

Prístupy & RBAC	Prevádzka (owner)
používateľské roly, práva na indexy/dashboards	SOC platform tím
roly pre tvorbu/spúšťanie workflow	SOC automation/engineering
roly/užívatelia (Wazuh UI/Elastic)	SOC endpoint tím
užívatelia/role v GVM	Vulnerability mgmt
roly/organizácie/práva	CTI tím
role-based prístup, sharing pravidlá	CTI tím
roly (IT/SOC/čítanie)	IT/Asset tím
roly/práva	Network/Infra tím
roly (analyst/lead/admin), prístup podľa case	SOC operations
role-based prístup, obmedzenia na citlivé prípady	DFIR/SOC tím
roly/dashboards permissions	SOC reporting
roly (read/edit/admin)	SOC knowledge owner

Poznámky / Riziká
Nároky na storage/performanciu; treba riešiť životný cyklus indexov a zálohy
Dôležité ošetriť tajomstvá (secrets), audit a schvaľovanie zásahov
Pokrytie agentmi a správne policy sú kritické; treba riešiť onboarding/offboarding endpointov
Community edícia môže mať limity v aktualizáciách/komforte; treba nastaviť okná skenov a dopad na sie
Dôležité nastaviť kvalitu zdrojov, deduplikáciu a “confidence”
Citlivé na správne nastavenie sharingu (čo sa môže zdieľať von)
Kvalita CMDB je kľúčová pre skeny a priorizáciu incidentov
Treba udržiavať aktuálnosť – inak skeny/monitoring míňajú cieľ
Dôležité je jednotné pomenovanie a workflow (stavové modely)
Treba nastaviť pravidlá práce s dôkazmi a citlivými dátami
Pozor na prístup k citlivým indexom; oddeliť view pre rôzne publikum
Udržiavať “single source of truth”; zaviesť proces revízie (napr. kvartálne)

ť

Oblasť / Funkcia (SOC)	Komponent (produkt)
SIEM	ELK Stack (Elasticsearch + Logstash/Beats + Kibana)
SOAR	Shuffle
EDR	Wazuh
Skener zraniteľností	Greenbone Community Edition (GVM)
CTI	OpenCTI
CTI	MISP
Asset management	GLPI
Asset management / IPAM/DCIM	NetBox
Ticketing	DFIR IRIS
Evidencia, správa incidentov	DFIR IRIS
Reporting	Kibana (ELK)
Knowledge portál	Wiki.js

Tok	Zdroj → Cieľ	Mechanizmus
EDR telemetry	Wazuh agents → Wazuh → ELK	natívna integrácia / ingest
Log ingestion	Zdroje logov → ELK	syslog/Beats → Logstash
Alert → SOAR	Wazuh/ELK → Shuffle	webhook/HTTP
CTI enrichment	Shuffle → OpenCTI	REST/GraphQL
IOC lookup	Shuffle → MISP	REST API
Case creation	Shuffle → DFIR IRIS	REST API
Asset context	Shuffle/IRIS → GLPI	REST API
Network context	Shuffle/IRIS → NetBox	REST API/webhook
Scan scope	NetBox → Greenbone	export/API
Vuln findings → ticket	Greenbone → DFIR IRIS/GLPI	export/API/automatizácia
Reporting	ELK → Kibana	interné v rámci stacku
Knowledge	DFIR IRIS → Wiki.js	manuálne alebo API

Formát/payload	Trigger/Frekvencia	Výstup
alert/event JSON	realtime	indexované udalosti + dashboards
syslog/JSON	realtime/batch	centralizované logy
JSON (alert)	pri alerte	spustený workflow
STIX-like entity/IOC query	on-demand v playbooku	enrichment do incidentu
attribute/event search	on-demand v playbooku	reputácia/tagy/IOC kontext
case/ticket JSON	pri relevantnom alerte	založený ticket/case
asset lookup	pri triage	owner/kritickosť/CMDB dáta
IP/device/site lookup	pri triage	IPAM/DCIM kontext
IP range/targets	plánovane	definované ciele skenu
report (JSON/CSV)	po skene	remediation ticket + evidencia
vizualizácie	priebežne	KPI/operatívne reporty
text/runbook	po uzavretí	aktualizované postupy